Trustworthy Computing: Securing Your Infrastructure

Scott Culp
Senior Security Strategist
Trustworthy Computing Team
Microsoft Corporation

THIRD ANNUAL

2003

Microsoft® STRATEGIC ARCHITECT FORUM

for Partners

Internet Has Changed Personal, Professional Ecosystems

- Began on PCs, but Now Across Many Devices
- Enhancements Have Been What Always Mattered
  - Productivity
  - Communication
  - Entertainment

...but adoption will stall unless people truly trust computer systems...

Framework for a Solution

Security Framework

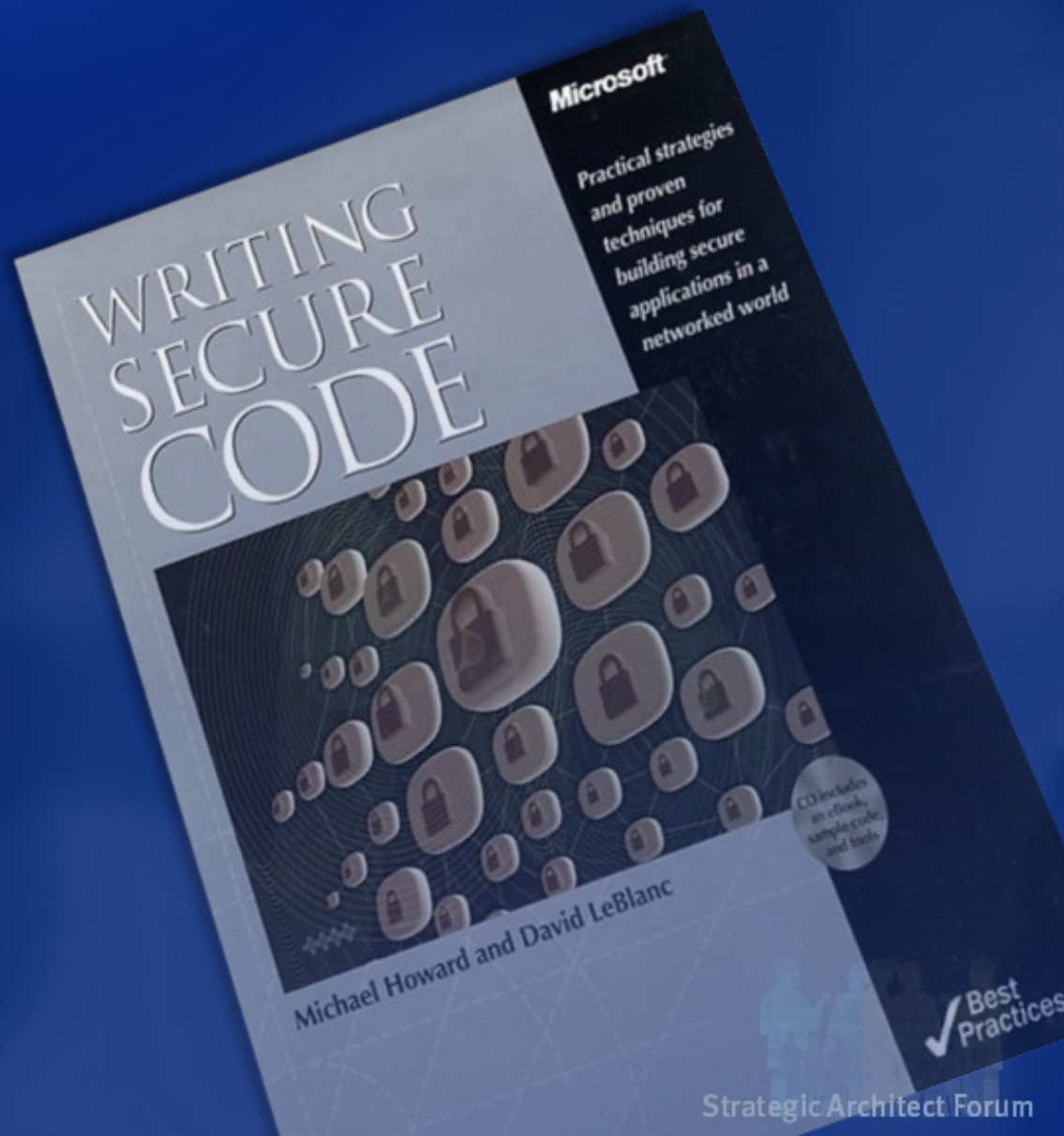
SD³ + Communication

Secure by Design	❖ Sound design and architecture ❖ Sound implementation
Secure by Default	❖ Smaller attack surface ❖ Better use of least privilege
Secure in Deployment	❖ Prescriptive guidance ❖ Simpler change management
Communication	❖ Formal commitment ❖ Timely, relevant information

Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication



Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication

Process

- **Mandatory security training for all developers**
- **Threat modeling, security reviews**
- **Extensive use of third-party reviews**

Products

- **Microsoft Windows Server™ 2003: New Internet Information Services (IIS) architecture**
- **Microsoft Office Exchange 2003: Improved antivirus API**
- **Microsoft Office System 2003: Native information rights management (IRM) support**
- **Microsoft Office Outlook® 2003: HTML content blocking**

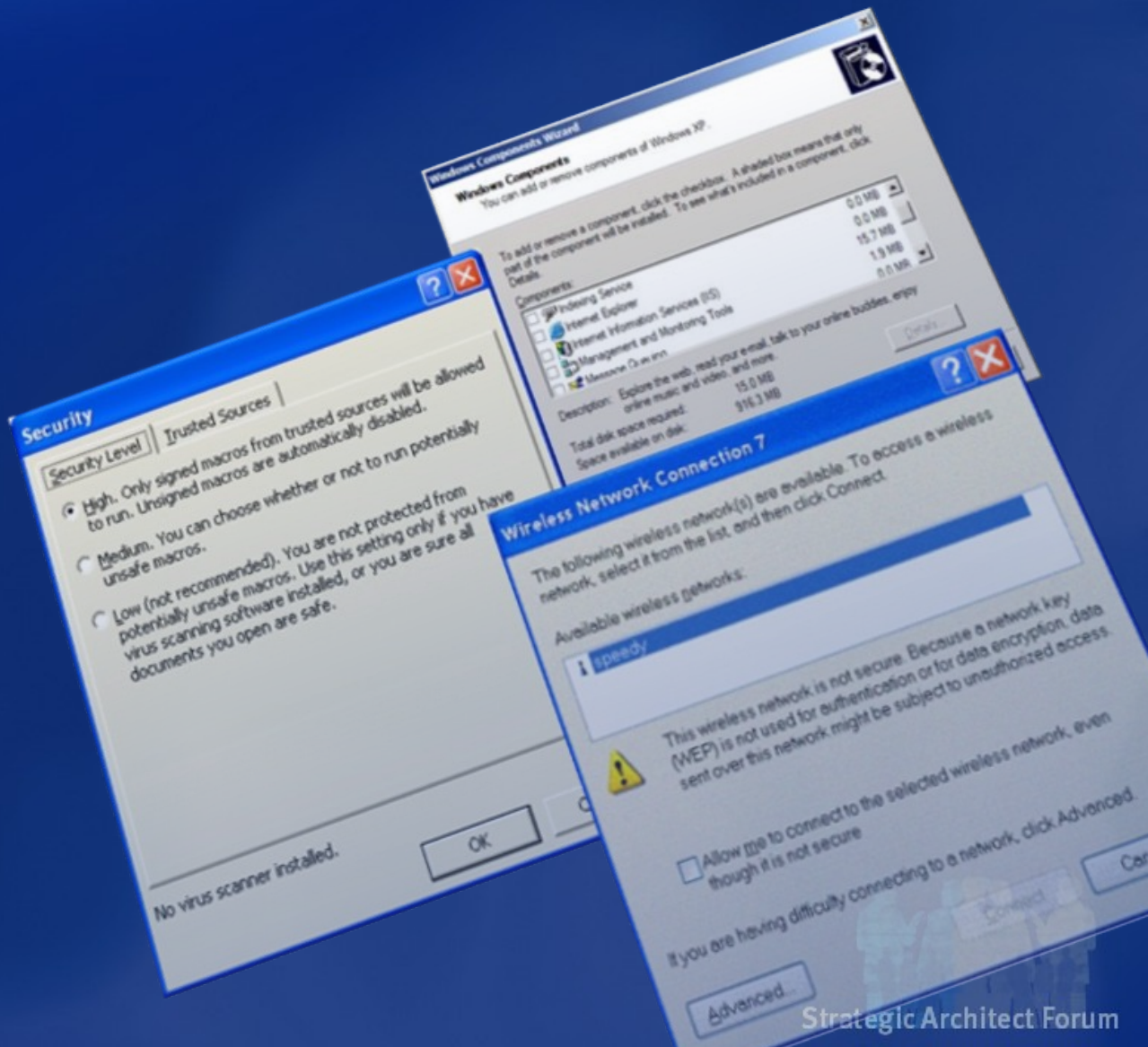
Investments

- **Next-Generation Secure Computing Base**

Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication



Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication

Windows Server 2003

- 60% reduction in attack surface
- IIS 6.0 neither installed nor running by default
- Blank password: No network authentication

Office System 2003

- Mail defaults to Restricted Sites Zone
- No trusted macro sources by default

Exchange 2003

- Less popular mail protocols disabled by default
- Microsoft Outlook Mobile Access (OMA) disabled by default

Defense In-Depth

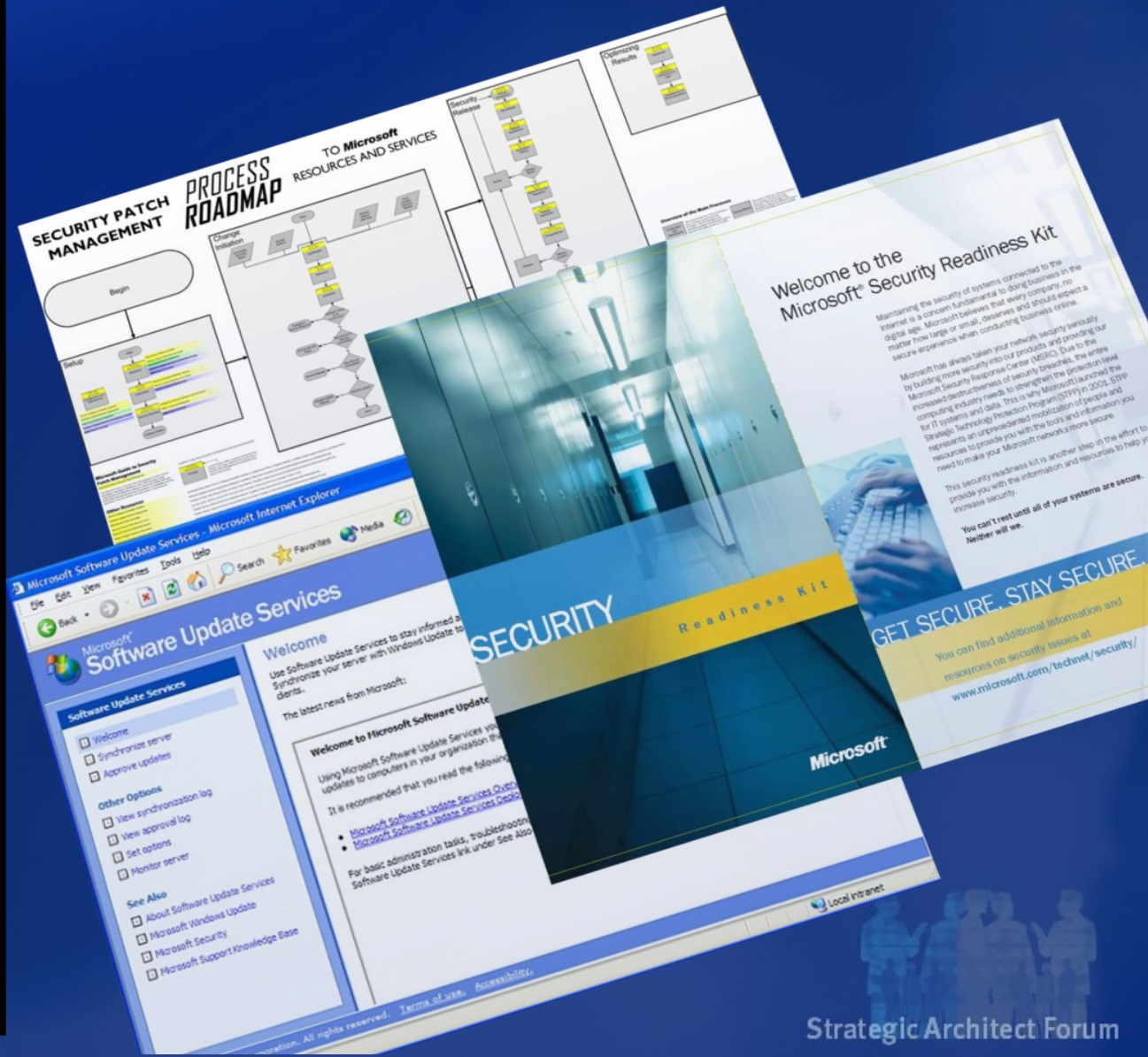
Microsoft Security Bulletin MS03-007: Buffer Overrun in DAV

Windows Server 2003 doesn't contain the flaw	Entire subsystem rewritten, quality improve
Even if it did contain flaw	IIS 6.0 not running by default
Even if IIS were running	IIS 6.0 doesn't have Distributed Authoring a Versioning (DAV) enabled by default
Even if DAV were enabled	Default URL length prevents exploitation
Even if none of the above safeguards existed	Would gain only "network service" privileges —commensurate with normal user

Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication



Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication

Prescriptive Guidance

- Reference architectures
- Patterns & Practices series
- Security Assessment Program (MCS/PSS)
- Common Criteria deployment guides

Tools

- Microsoft Windows® Update, Microsoft Office Update
- URLScan, IIS Lockdown, SQL security tools
- Microsoft Baseline Security Analyzer (MBSA), Microsoft Software Update Services (SUS), and Microsoft Systems Management Server (SMS) Feature Pack
- SMS 2003

You've Told Us...

"The quality of the patching process is low and inconsistent"

"I need to know the right way to run a Microsoft enterprise"

"I can't keep up... new patches are released every week"

"There are still too many vulnerabilities in your products"

Our Action Items:

Improve the patching experience

Provide guidance and training

Mitigate vulnerabilities without patches

Continue improving quality

Improve the Patch Experience

Operational Improvements

Security
Support
Monthly
Patches

- Microsoft Windows 2000 SP2: June 2004
- Microsoft Windows NT® 4.0 Workstation SP6a: June 2004
- Predictability
- Patch consolidation

OTE: Out-of-cycle patches may be released as necessa
protect customers under active attacks

Improve the Patch Experience

Technical Improvements

Reduce Complexity

- One patch experience
- Convergence on proven technologies

Reduce Risk

- Better quality patches
- Rollback capability for all patches

Reduce Size

- 30-80% smaller patches through delta patching

Reduce Downtime

- 10-30% fewer reboots than last year

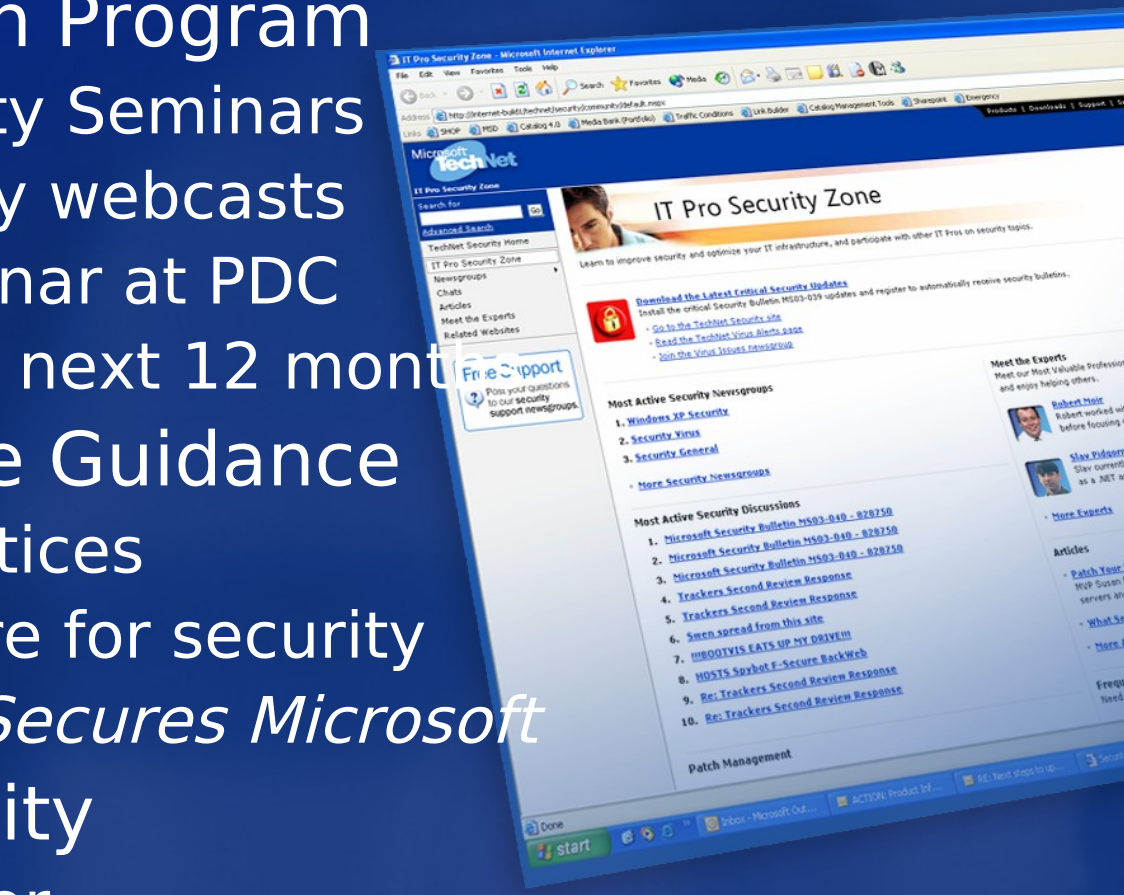
Extend Automation

- SUS 2.0
- SMS 2003
- Windows Update > Microsoft Update

Windows 2000+ Generation by May 2004

Guidance and Training

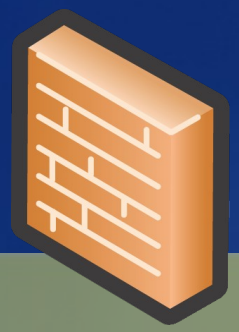
- Global Education Program
  - TechNet Security Seminars
  - Monthly security webcasts
  - Dedicated seminar at PDC
  - 500,000 people next 12 mont
- New Prescriptive Guidance
  - Patterns & Practices
  - How to configure for security
  - *How Microsoft Secures Microsoft*
- Online Community
  - Security Zone for IT professionals



Mitigating Vulnerabilities

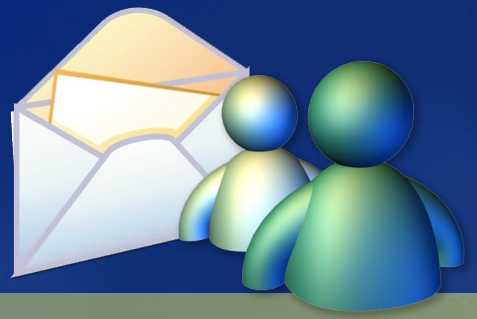
Safer Networking	Internet Connection Firewall on by default; centrally managed, improved compatibility
Safer E-Mail and IM	More secure default settings; Improved attachment blocking
Safer Browsing	Better protection against malicious code; user controls to prevent malicious Microsoft ActiveX® controls and Spyware
Improved Memory Protection	Compiler checks (/GS) to reduce stack overruns; hardware protection to block heap overrun protection
Perimeter Inspection	Enforce corporate security standards; only safe clients can connect

Safer Networking



What It Is	Microsoft Windows XP Internet Connection Firewall
What It Does	Helps stop network-based attacks, like Blaster, by closing unnecessary ports
Key Features	❖ Protection turned on by default ❖ Improved interface makes it easier to configure ❖ Improved application compatibility ❖ Enhanced enterprise administration through Group Policy

Safer E-mail and IM



What It Is	Improved protection against malicious e-mail attachments and IM file transfers
What It Does	Helps stop viruses that spread through e-mail messages and IM, like SoBig.F
Key Features	❖ More secure default settings ❖ Improved attachment blocking for Microsoft Outlook Express and IM ❖ Increased Outlook Express security and reliability

Safer Browsing

What It Is	Safer browsing using Microsoft Internet Explorer
What It Does	Improved protection against malicious content on the Web
Key Features	❖ Better protection against harmful Web downloads ❖ Better user controls to prevent malicious ActiveX controls and Spyware ❖ Reduced potential for Internet Explorer buffer overruns

Improved Memory Protection

What It Is	Reduction of potential buffer overruns
What It Does	Helps prevent the execution of malicious code in memory normally reserved for data
Key Features	❖ Improved compiler checks (/GS) to reduce stack overruns ❖ Improved heap overrun protection ❖ Leverages new processor innovations (NX) to prevent stack and heap overruns

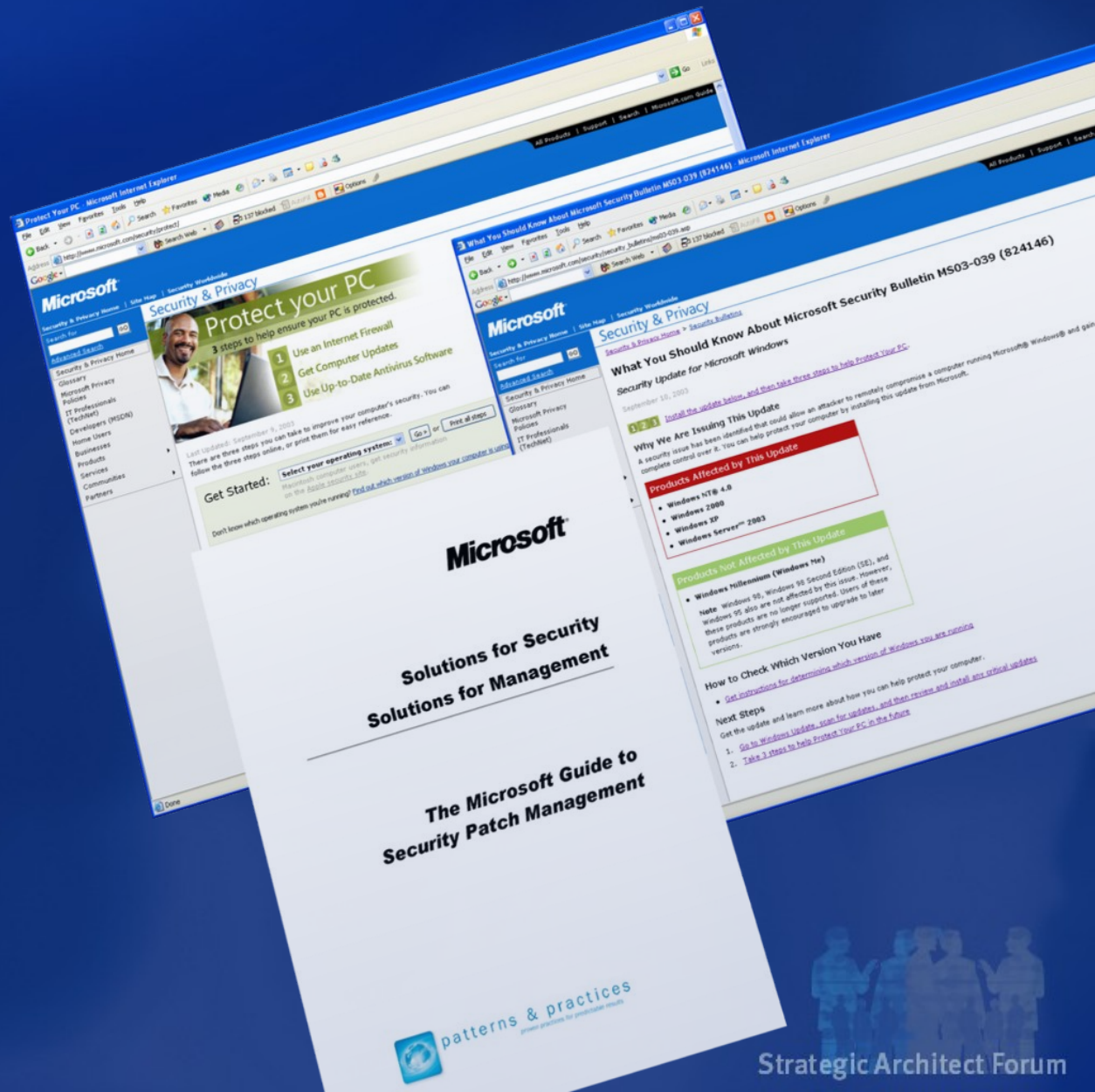
Perimeter Inspection

What It Is	Only clients that meet corporate security standards are allowed to connect Included in Windows Server 2003 SP1 (H204); more to follow
What It Does	Protects enterprise assets from infected computers
Key Features	❖ Role-based config to lockdown servers ❖ Enforces specific corporate security requirements such as patch level, AV signature state, and firewall state ❖ Ensure these standards are met when: ◆ Virtual Private Networking (VPN) connections are made by remote clients ◆ Wired or wireless connections are

Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication



Progress to Date

SD³ + Communication

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication

Security Response Center

- Tailored content for IT pros, home users
- More effective response to Internet attacks
- Protect Your PC campaign

Improved Support for Developers

- “Writing Secure Code”, Second Edition
- MSDN® security guidance

Community Outreach

- Critical infrastructure protection
- Law enforcement
- Security community

TWC Life Cycle

Design Docs and Specifications 	Design	Security Review	❖ Each component team develops threat models, ensuring that design blocks applicable threats
Development, Testing, and Documentation 	Development: M1	Develop and Test	❖ Apply security design and coding standards ❖ Tools to eliminate code flaws (PREfix and PREfast)
	Development: M2		
	Development: Mn	Security Push	❖ Monitor and block new attack techniques ❖ Team-wide stand down ❖ Threat model updates, code review, test, and documentation scrub
	Development: Beta		
Product 	Release	Security Audit	❖ Analysis against current threats ❖ Internal and third-party penetration testing
Service Packs, QFEs 	Support	Security Response	❖ Fix newly discovered issues ❖ Root cause analysis to proactively find and fix related vulnerabilities

Security Roadmap

2003

- Extended Support
- Monthly Patch Releases
- SMS 2003
- Baseline Guidance
- Community Investments

H1 04

- Windows XP SP2
- Patching Enhancements
- SUS 2.0
- Microsoft Update
- Broad Training

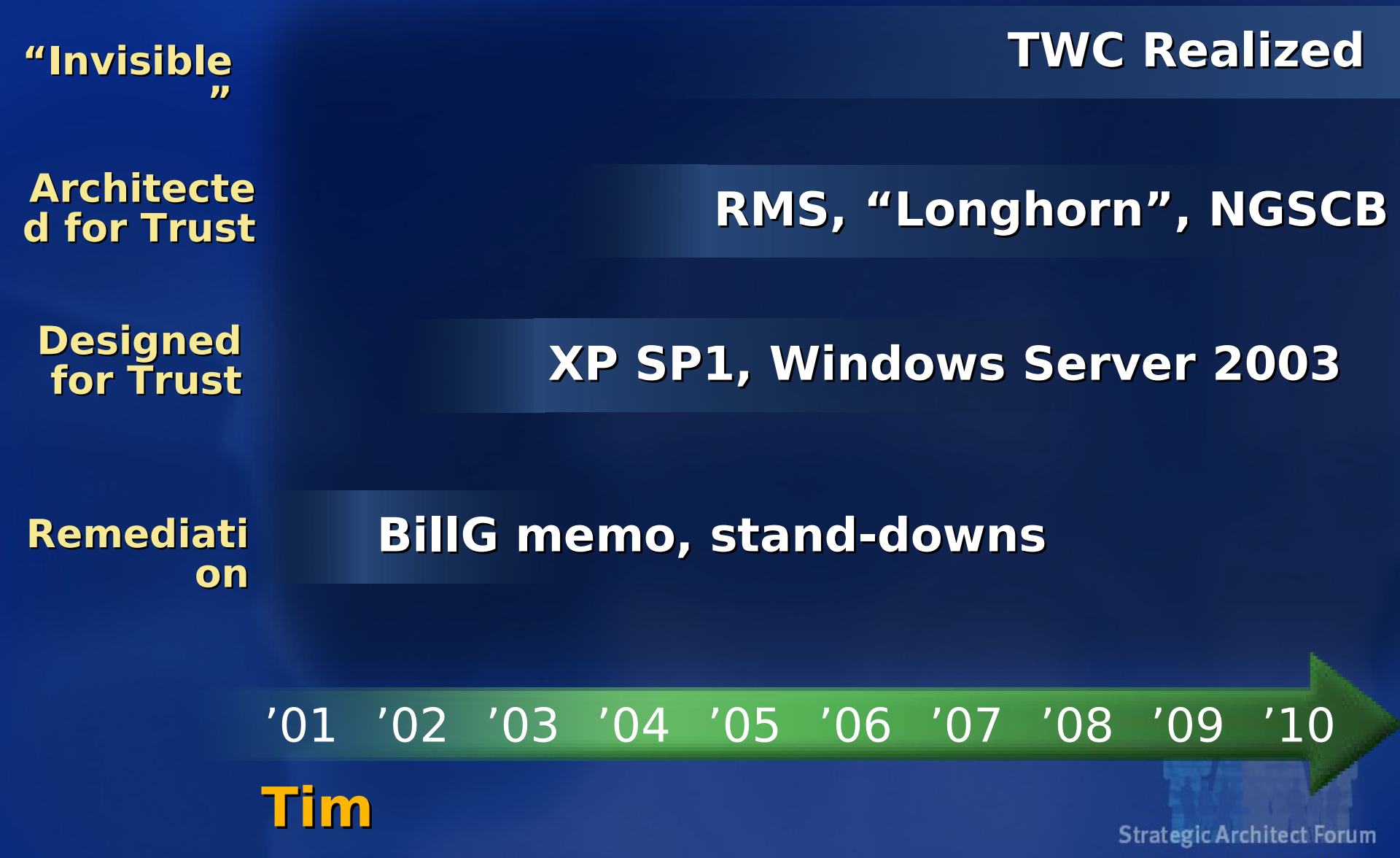
H2 04

- Windows Server 2003 SP1
- Next-Generation Inspection

Future

- Next-Generation Secure Computing Base (NGSCB) Windows Hardening
- Continued Safety Technologies

A Long Journey



Questions?

Microsoft®

Reading List

Support Life Cycle	http://support.microsoft.com/default.aspx?scid=fh;%5bln%5d;complifeport
Writing Secure Code	http://search.barnesandnoble.com/booksearch/isbninquiry.asp?ISBN=0735615888
Five-Minute Security Advisor	http://www.microsoft.com/TechNet/Columns/Security/5Min
Security Notification Service	http://www.microsoft.com/technet/security/bulletin/notify.asp
IT Showcase	http://www.microsoft.com/technet/itsolutions/msit
Windows 2000 Common Criteria	http://www.microsoft.com/technet/security/issues/w2kccwp.asp
OIS Vulnerability Handling Guidelines	http://www.oisafety.org/reference/process.pdf
Microsoft Security Response Policy	http://www.microsoft.com./technet/security/bulletin/msrpracs.asp

Reading List

Guide to Security Patch Management	http://www.eu.microsoft.com/technet/security/topics/patch/secpatch
Patch Standardization	http://www.microsoft.com/technet/security/topics/patch/stdpatex.asp
Prescriptive Architecture Guide	http://www.microsoft.com/technet/itsolutions/edc/pak
Patterns & Practices	http://www.microsoft.com/resources/practices/completelist.asp
Exchange 2003 Security	http://www.microsoft.com/exchange/evaluation/Security_e2k3.asp
Windows 2003 Security Guide	http://www.microsoft.com/technet/security/prodtech/windows/win2003/w2003hg/sgch00.asp
Outlook 2003 Security	http://www.microsoft.com/technet/prodtechnol/office/Office2003/Plan/O3secdet.asp
Windows XP SP2: Developers Guide	http://msdn.microsoft.com/library/en-us/dnwxp/html/securityinxpsp2.asp

Tools

Outlook E-Mail Security Update	http://office.microsoft.com/downloads/2000/Out2ksec.aspx
IIS Lockdown Tool and URLScan	http://www.microsoft.com/technet/security/tools/tools/locktool.asp
Microsoft SQL Server™ Security Tools	http://www.microsoft.com/SQL/downloads/securitytools.asp
Microsoft Baseline Security Analyzer	http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp
Software Update Services	http://www.microsoft.com/windows2000/windowsupdate/sus
SMS 2.0 Feature Packs	http://www.microsoft.com/smserver/evaluation/overview/featurepacks